ABSTRACT

A system, apparatus, and method are provided for enhancing entropy in a pseudo-random number generator (PRNG) using remote sources. According to one embodiment of the present invention, first, the PRNG's internal state is initialized. Local seeding information is then obtained from a local host. For added security, additional seeding information is obtained from one or more remote entropy servers operating independently to each maintain a constantly updated state pool. Finally, the PRNG is stirred based upon the local seeding information, and the additional seeding information.